IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Bardsley et al.**	§	
	§	Group Art Unit: **2137**
Serial No. **09/917,368**	§	
	§	Examiner: **Popham, Jeffrey D.**
Filed: **July 27, 2001**	§	
	§	Confirmation No.: **1486**
For: **Correlating Network Information and Intrusion Information to Find the Entry Point of an Attack Upon a Protected Computer**	§	

37945

PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF (37 C.F.R. 41.41)

This Reply Brief is submitted in response to the Examiner's Answer mailed on February 5, 2008.

No fees are believed to be required to file a Reply Brief. If any fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0457.

RESPONSE TO EXAMINER'S ANSWER

A. 35 U.S.C. § 102, Alleged Anticipation of Claims 5-11, 15, and 18-20

With regard to claim 5, Appellants respectfully disagree with the Examiner's assertions that the *Ricciulli* reference teaches the features of (1) "determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information", and (2) "identifying a physical entry point associated with the logical entry point".

With respect to "determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information," the Examiner states:

> How the determining step works is further shown by claim 10, in that "the step of determining a logical entry point includes the step of finding, in the network information, the logical port identifier of the logical port associated with the address." This logical port identifier is included in the network information (claim 9, from which claim 10 depends). Therefore, determining the logical entry point comprises finding the logical port identifier within the network information. Ricciulli (Figure 3, and column 4, line 45 to column 5, line 2, for example), explicitly shows finding, in the list(s) of network information, the logical port associated with the attack. This is performed by matching the intrusion information to the list(s) of network information to determine if a correlation is found. Ricciulli describes that "There are many possible network characteristics that can be matched in 3150. For example, IP source addresses 330, destination IP addresses 335, source TCP ports 340, source UDP ports 345, destination TCP ports 350, destination UDP ports 355, TCP flags 360, and/or ICMP flags 365" (column 4, line 65 to column 5, line 2). As seen here, any or all of this information may be correlated between the intrusion information and the list(s) of network information, this information including TCP and UDP ports, which Appellant admits are logical entry points (page 17, for example). Since more limiting claim 10 describes the determining step as finding the logical port identifier of a logical port within the network information, and Ricciulli teaches finding the logical port identifier of a logical port within the list(s) of network information, Ricciulli must teach the broader determining step of claim 5.
>
> After this determining is completed within Ricciulli, the most upstream device that had seen the attack traffic (and implements the system) is identified as the physical entry point. Since this physical entry point had seen the attack traffic and had network information regarding such traffic in its list(s)/cache, that physical device/entry point must be associated with the logical entry point that was determined as just described. As described below, the physical entry point may be either the current node or the downstream neighbor, as shown in column 3, lines 39-47.

> Once this physical entry point is found, filtering may be put into place on such physical device/entry point. This is shown in column 3, lines 57-58 and column 4, lines 50-61. Column 3, lines 57-58 shows that, in one embodiment, "Filtering rules can be dynamically installed on an identified entry point", and the column 4 section shows more details about such filtering. Since such filtering rules are installed on an identified entry point, the entry point must have been identified, and it must be a physical entry point since the filtering rules are installed on the entry point. This physical entry point on which the filtering rules may be installed is associated with the logical entry point, as described above.

(Examiner's Answer dated February 5, 2008, pages 12-14.)

Contrary to the Examiner's assertions above, the sections cited by the Examiner still do not teach determining a logical entry point of an attack by correlating the intrusion information and the network information. Although *Ricciulli* discloses in column 4, line 65 to column 5, line 2 that a network characteristic list that may contain TCP and UDP port information, *Ricciulli* does not teach that a correlation of intrusion information and the network information is used to determine a logical entry point of an attack. The section of *Ricciulli* cited by the Examiner (column 4, line 45 to column 5, line 2) merely teaches that messages are initially prevented from transiting a first network node. "Suspicious instances" in the messages are compared with repeated updated lists of network characteristics. In particular, column 4, lines 57-59 of *Ricciulli* states, "In **315**, suspicious instances can be compared with repeatedly updated lists. If the compare fails to result in a match, prevention can be halted." Consequently, if the "suspicious instance" in the message does not match the network characteristics in the list, then the message is allowed to transit the first network node. However, there is no explicit teaching in the cited section of *Ricciulli* of correlating intrusion information and network information to determine a logical entry point of an attack. Instead, the cited section of *Ricciulli* teaches comparing a suspicious instance in a message to a list of network characteristics to find a match. If such a match is found from the comparison, the message is allowed to pass from the first network node to the next network node.

The Examiner alleges that since claim 10 of the present invention describes the determining step as finding the logical port identifier of a logical port within the network information, *Ricciulli* must teach the broader determining step of claim 5 because the Examiner states that *Ricciulli* teaches finding the logical port identifier of a logical port within the list(s) of network information. However, obtaining port information from a message and comparing that port information to source

and destination port information in a network characteristics list is still not the same as determining a logical entry point of an attack. As evident in column 3, lines 16-43, *Ricciulli* merely teaches identifying a physical entry point of the attack as the router which did not have a host address in its cache as the source of the attack. Despite the Examiner's allegations, the cited section of *Ricciulli* makes no mention of determining a logical entry point of an attack, nor of making this determination by correlating intrusion information and network information using a correlation engine.

In addition, the sections cited by the Examiner still do not teach identifying a physical entry point associated with the logical entry point. As evident in column 4, line 45 to column 5, line 2 and column 3, lines 16-47, *Ricciulli* merely teaches identifying a physical router as the source of attack. Specifically, column 3, lines 39-43 states "…if an upstream router does not find H in the local cache, a report message can be sent to R with, for example, interface information of a downstream neighbor and the cookie. In some embodiments, this can be identified as an entry point of the attack, such as the flood". Column 3, lines 44-47 of *Ricciulli* further states "If the upstream router does not implement this mechanism the router will send a report packet to R with its interface information and/or the cookie (this will be identified as the entry point of the flood)." According to the Examiner, the interface information identifies the physical entry point of the flood (Examiner's Answer, page 16, line 14). Thus, *Ricciulli* merely discloses finding the physical entry point of an attack – the router lacking a host address in a cache. As *Ricciulli* has been shown as failing to teach determining the logical entry point of an attack, there can be no subsequent teaching in *Ricciulli* of identifying a physical entry point associated with such a logical entry point of the attack.

The Examiner also argues that an IP address is a logical address used to identify the device, and since the device can be considered a physical entry point and the IP address can be a logical address associated with the physical device, the IP address must be a logical entry point. (Examiner's Answer, page 14.) Appellants respectfully disagree. There is no such teaching in *Ricciulli* that an IP address must be a logical entry point. Rather, as stated by the Examiner, an IP address is a logical address used to identify the device. The IP address merely represents a single machine connected to the Internet. An IP address is merely an identifier of a device, not a point of entry to the device.

The Examiner also argues the relevancy of whether or not IP addresses and TCP/UDP ports are logical entry points. (Examiner's Answer, page 15.) The Examiner's assertion in the Office Action of June 12, 2007, p. 4 alleged that "IP addresses, as well as TCP/UDP ports are logical representations used in combination to identify the entry point". However, this assertion is not supported by the teachings of *Ricciulli*. The Examiner makes the assumption that since *Ricciulli* teaches identifying an entry point, the mention of IP addresses and TCP/UDP ports in *Ricciulli* leads to identifying a logical entry point. However, as previously discussed, *Ricciulli* only teaches finding a physical entry point of an attack. Also, contrary to the Examiner's assertion, *Ricciulli* is not "entirely concerned with determining and identifying entry points of an attack, as seen throughout the description." Rather *Ricciulli* is concerned with "maintaining lists of network characteristics of messages" and updating these lists as needed, as described in the Abstract, Summary, and Claims, which do not mention anything about a concern for determining and identifying entry points of an attack.

The Examiner also argues that the interface information sent in the response of a router which does not find the network/host address in its local cache identifies a physical entry point (interface information) associated with the logical entry point (i.e., IP address). Again, the Examiner is attempting to equate an IP address with a logical entry point of a device and thus claim that *Ricciulli* teaches determining a logical entry point of an attack. However, it is the Examiner who is relying on faulty logic in asserting that *Ricciulli* teaches an IP address is a logical entry point of a device. As previously stated, *Ricciulli* does not teach determining a logical entry point of a device or making such a determination by correlating intrusion information and network information. An IP address allows for reliably identifying a device in a network, but does not provide a logical point of entry to the device.

CONCLUSION

As shown above, *Ricciulli* does not anticipate the claims. Similarly, the Examiner has failed to state a *prima facie* obviousness rejection against the claims. Therefore, Appellants request that the Board of Patent Appeals and Interferences reverse the rejections. Additionally, Appellants request that the Board direct the Examiner to allow the claims.

/Cathrine K. Kinslow/

Cathrine K. Kinslow
Reg. No. 51,886
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777